USCYBERCOM AND CYBER SECURITY: IS A COMPREHENSIVE STRATEGY POSSIBLE?

BY

COLONEL MICHAEL P. JACKSON
United States Army

USAWC CLASS OF 2011

U.S. Army War College, Carlisle Barracks, PA 17013-5050

REPORT DOCUMENTATION PAGE

1. REPORT DATE *(DD-MM-YYYY)* 12-05- 2011	2. REPORT TYPE Program Research Project		3. DATES COVERED *(From - To)*
4. TITLE AND SUBTITLE USCYBERCOM and Cyber Security: Is a Comprehensive Strategy Possible?			5a. CONTRACT NUMBER
			5b. GRANT NUMBER
			5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) COL Michael P. Jackson			5d. PROJECT NUMBER
			5e. TASK NUMBER
			5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Dr. Jeff Groh Department of Distance Education			8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army War College 122 Forbes Avenue Carlisle, PA 17013			10. SPONSOR/MONITOR'S ACRONYM(S)
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
In 2008, after a significant breach of its networks, the Department of Defense realized that a military so heavily reliant on cyberspace is also vulnerable to anyone with access to the Internet. With all the national strategic guidance, USCYBER Command has yet to develop a comprehensive strategy. USCYBERCOM must create a strategy that fosters unity of effort and action to operate successfully in the cyber domain. This paper will examine five aspects of US Cyber Command: organization, command and control, computer network operations (CNO), synchronization, and resourcing. It will identify areas that currently present significant risk to USCYBERCOM's ability to create a strategy that can achieve success in its cyberspace operations. This paper will recommend potential solutions that can improve the USCYBERCOM strategy to advance the nation's security posture in cyberspace.

15. SUBJECT TERMS
Computer network operations, CNO, computer network attack, CNA, Computer Network Exploitation, CNE, cyberspace, cyber, cyberspace operations, cyber defense, National Security Strategy, NSS, National Military Strategy for Cyberspace Operations, NMS-CO, information operations, IO, United States Code Title 50, Title 10

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT UNCLASSIFED	b. ABSTRACT UNCLASSIFED	c. THIS PAGE UNCLASSIFED	UNLIMITED	28	19b. TELEPHONE NUMBER *(include area code)*

USAWC PROGRAM RESEARCH PROJECT

USCYBERCOM AND CYBER SECURITY: IS A COMPREHENSIVE STRATEGY POSSIBLE?

by

Colonel Michael P. Jackson
United States Army

Project Adviser
Dr Jeffrey L. Groh
Faculty Instructor

This PRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Michael P. Jackson

TITLE: USCYBERCOM and Cyber Security: Is a Comprehensive Strategy Possible?

FORMAT: Program Research Project

DATE: 12 May 2011   WORD COUNT: 5,081   PAGES: 28

KEY TERMS: Computer network operations, CNO, computer network attack, CNA, Computer Network Exploitation, CNE, cyberspace, cyber, cyberspace operations, cyber defense, National Security Strategy, NSS, National Military Strategy for Cyberspace Operations, NMS-CO, information operations, IO, United States Code Title 50, Title 10

CLASSIFICATION: Unclassified

In 2008, after a significant breach of its networks, the Department of Defense realized that a military so heavily reliant on cyberspace is also vulnerable to anyone with access to the Internet. With all the national strategic guidance, USCYBER Command has yet to develop a comprehensive strategy. USCYBERCOM must create a strategy that fosters unity of effort and action to operate successfully in the cyber domain. This paper will examine five aspects of US Cyber Command: organization, command and control, computer network operations (CNO), synchronization, and resourcing. It will identify areas that currently present significant risk to USCYBERCOM's ability to create a strategy that can achieve success in its cyberspace operations. This paper will recommend potential solutions that can improve the USCYBERCOM strategy to advance the nation's security posture in cyberspace.

USCYBERCOM AND CYBER SECURITY: IS A COMPREHENSIVE STRATEGY POSSIBLE?

Since the turn of this century, the cyber environment developed into one of the nation's most significant security interests. The fact that the nation's elements of power, diplomacy, information, military and the economy (DIME) are significantly dependent on information systems connected to the global internet leaves them increasingly vulnerable to threats from not only adversaries, but non-state and criminal elements as well. In the late 1990's, the United States government began efforts to develop a strategy to defend this significant security interest. The Department of Defense, predominantly through its intelligence community and the Air Force[1], began to develop concepts and guidance on computer network operations (CNO). For the last 20 years, the Department has undergone one of its most significant transformations; harnessing the capabilities of the Internet to create a network-centric military for the 21stcentury. Unfortunately, the elements of CNO; Computer Network Defense (CND), Computer Network Attack (CNA) and Computer Network Exploitation (CNE), were developing separately from each other, with CNA and CNE buried deep behind highly classified doors. In 2008, after a significant breach of its networks, the Department realized that a military so heavily reliant on cyberspace is also vulnerable to anyone with access to the Internet.

Today, security of cyberspace has become one of the most significant and complex issues facing the nation. Without an effective holistic strategy that can unify and provide viable deterrence the nation will continue to remain vulnerable. On July 23 2009, the Pentagon ordered the creation of US CYBER Command as a Sub-unified Command under USSTRATCOM.[2] The intent was to harness the divergent

organizations and elements of the Department that operate in the cyber domain under one command. With all the national guidance and strategy, USCYBERCOM has yet to develop a comprehensive strategy. USCYBERCOM must create a strategy that fosters unity of effort and action to operate successfully in the cyber domain. This paper will examine five aspects of US Cyber Command: organization, command and control, computer network operations (CNO), synchronization, and resourcing. It will identify areas that currently present significant risks to USCYBERCOM's ability to create a strategy that can achieve operational success in cyberspace. This paper will recommend potential solutions that can increase effectiveness of the USCYBERCOM strategy to advance the nation's security posture in cyberspace.

Developing the Need for USCYBERCOM

In the 1990s, the DOD began transforming into a network-centric organization heavily dependent on cyberspace to carry out its military strategy, but it did not grasp the significance of addressing cyber-security issues until after vulnerabilities appeared. "In 1998, a presidential commission reported that protecting cyberspace would become crucial… To meet this new threat, we have relied on an industrial age government and an industrial age defense."[3] In 2003, President Bush signed the *National Strategy to Secure Cyberspace* (NSSC)[4] outlining five national priorities and placing much of the security burden on the Department of Homeland Security (DHS). From April to June 2007, intrusions into several government departments; DoD, National Aeronautics and Space Administration, Energy, Commerce, and State by unknown attackers resulted in the loss of 20 terabytes of data.[5] In the period from 2006 to 2008 reported cyber

incidents more than tripled,[6] supporting a growing opinion that the nation remained at risk and had yet to address the priorities it recommended in the 2003 NSSC.

Although cyber security has been a topic of discussion since the 1990s, the word "cyber" in U.S. national security strategic documents is a relatively new term. The *National Security Strategy* (NSS) of 2002 does not mention it at all. The *National Security Strategy* of 2006 uses it just once to describe one of several disruptive threats to national security.[7] By 2010, the National Security Strategy uses the word cyber or cyberspace 23 times with a mention in the table of contents as well.[8] In 2006, other documents began to address cyberspace. The *Quadrennial Defense Review* of that year directed resource investment and improved coordination regarding cyber and network security.[9] Also in 2006, the DoD published the *National Military Strategy for Cyberspace Operations*.[10] It assigned USSTRATCOM, with the Joint Staff as a co-lead, to develop an implementation plan within 60 days, including terms of reference and specific tasks lists with assigned lead agencies.[11] After the US incidents in 2007 and a series of international cyber offensive incidents in 2007-2009, including Estonia, Georgia and North Korea, cyberspace gained the public's attention. The 2008 report *Securing Cyberspace for the 44th Presidency* from the Center for Strategic and International Studies (CSIS), determined that the nation needed to move toward a whole of government approach as a solution. Its three major findings were, "(1) cyber security is now a major national security problem for the United States, (2) decisions and actions must respect privacy and civil liberties, and (3) only a comprehensive national security strategy that embraces both domestic and international aspects of cyber security will make us more secure."[12] The document called for the DoD to stay

involved but not take the lead to avoid risking a militarization of cyber space.[13] In a 2009 response to congressional inquiries, the White House commissioned the "*Cyberspace Policy Review*", which identified that the U.S. had failed to keep pace with the threat and called for a "comprehensive framework to ensure a coordinated response by federal, state, local and tribal governments, the private sector and international allies…"[14]

The DoD, in its 2006 *National Military Strategy for Cyberspace Operations,* recognized that cyberspace, with all its complexities and vulnerabilities, was a warfighting domain.[15] Cyberspace is also a domain "without a primary Service as lead…"[16] Over time, several organizations, predominately the Service communicators and the national intelligence community, developed cyberspace capabilities but they were unsynchronized, tended to have limited focus within their physical domains or functional areas, and were mostly independent of each other. In 2008, the DoD stopped an early attempt by the US Air Force to stand up a Cyberspace Command based on its belief that the mission to defend the U.S. military networks belonged in U.S. Strategic Command rather than a single service or agency.[17] Within a year, on 23 Jun 2009, Secretary of Defense Gates signed the order authorizing the establishment of USCYBERCOM. To address the risk posed by cyberspace,

> …the Department of Defense requires a command that possesses the required technical capability and remains focused on the integration of cyberspace operations. Further, this command must be capable of synchronizing warfighting effects across the global security environment as well as providing support to civil authorities and international partners.[18]

This order did three things. First, it re-emphasized cyberspace as a warfighting domain and second, that the DoD must be ready to conduct operations in it. Third,

unfortunately, it left out clear intent, scope and concept of operations. This has left USCYBERCOM to interpret and negotiate how to shape these disparate cyber elements together and develop a successful strategy.

Organizational Structure

The basic organizational structure of USCYBERCOM has three weaknesses. The first weakness is that the base order establishing USCYBERCOM only "reinforced" and did not expand USSTRATCOM's authorities and responsibilities for military cyberspace.[19] The USSTRATCOM transitioned its responsibilities to USCYBERCOM, a sub-unified command. In general, a sub-unified command carries a reduced level of authority in the DoD command structure.[20] Though too early to tell, USCYBERCOM may not have the authority to synchronize fully across the Services and the other combatant commands (CCMDs). Due to the very nature of the cyberspace domain in which USCYBERCOM operates, this limitation could continue to produce vulnerabilities. This leads to the second organizational structure concern. Instead of organizing the command to align regionally across the globe, the department structured the command along Service lines, adding subordinate Service commands to its structure. COL David Hollis, in an article arguing for USCYBERCOM to be its own CCMD, points out that with no one Service responsible to protect cyberspace like other warfighting domains (air, land, and sea), as a sub-unified command USCYBERCOM lacks the authorities and responsibilities to compensate.[21] In addition, as a sub-unified command organized along Service structures, resourcing becomes a central issue for USCYBERCOM. In order for the organization to achieve unity of effort, it is reliant on the Services to accept direction and agree to fund the global initiatives needed to standardize the tools,

capabilities, and skilled force structure desired by USCYBERCOM. The last structural

weakness is the dual-hatting of the commander.

Currently the Director of NSA (DIRNSA) is also the commander of

USCYBERCOM. This brings into question whether or not a single commander can pay

adequate attention to critical, immediate and diverse responsibilities of two

organizations. Though dual-hatted command responsibilities are commonplace in joint

operations and within other DoD organizations, there is the perception that staff

responsibilities and resources could be misaligned, thereby reducing effectiveness of

one command or the other. In recent testimony to Congress, General Alexander

discussed this point, reassuring the committee that with the collocation of

USCYBERCOM and NSA/CSS, the core missions of NSA/CSS will not change with the

continued growth of USCC.[22] With the complexities of the command and control

relationships within the Department of Defense, the dual-hatting of a combat support

agency over a sub-unified command further dilutes command relationships and unified

action, increasing the burden of continuous coordination as described in Joint

Publication 1(JP1).[23] The next aspect of USCYBERCOM, command and control, will

explore the inherent weaknesses a sub-unified command must overcome to meet the

security challenges of the cyberspace domain.

Command and Control

The complexity of the global cyberspace domain, uncoordinated guidance,

fragmented doctrines, and the disparate organizations that define computer network

operations (CNO) denote just a few of the impediments to effective command and

control USCYBERCOM will need to overcome. The issue of command and control (C2)

authorities and responsibilities is not a new concern for functional component

commands (FCC). For a sub-unified combatant command, the challenge is even more

significant. To be successful it must achieve legitimacy, authority, and influence from its

position within the DoD command structure. It must be value added. This will require

constant engagement and coordination with the interagency, DoD support agencies,

geographic combatant commands, the four FCCs, the Services, and joint staff to

achieve success and, "ensure U.S. and allied freedom of action in cyberspace."[24] Since

its inception, USCYBERCOM has also fought concerns over civil liberties and other

issues that delayed its establishment of initial operating capability (IOC), and many of its

missions, relationships, and authorities remain unresolved.[25] Second causes for

concern are the independent Service based cyber structures and how USCYBERCOM

will exercise command and control over its constituent units.[26]

Two recent articles by COL David Hollis in 2010 and one by Major M. Bodine

Birdwell just recently published in the *Air and Space Power Journal*, present different

approaches to transition USCYBERCOM into a full CCMD modeled after USSOCOM.

Both believe that the creation of USCYBERCOM is a good first step, but that the DoD

should pursue transitioning it into a full functional combatant command. Both authors

seek a single organization with the authority to provide C2, coordination, and the

authority to synchronize cyber capabilities over the entire DoD and perhaps more. In his

article, Birdwell limits the scope of USCYBERCOM's responsibilities to the DoD.[27] Hollis

envisions a broader scope of responsibility, to include the entire government and

perhaps the nation.[28] Both believe the current sub-unified construct under

USSTRATCOM needs fundamental change to overcome command and control issues

with the Geographic Combatant Commands (GCC). In a separate thesis, Birdwell

believes that adapting tested doctrinal solutions implemented by CCDRs

(i.e.USSTRATCOM, USTRANSCOM, and USSOCOM) can resolve issues with

authorities, coordination and synchronization between USCYBERCOM and the GCCs

over Service cyber capabilities.[29] Due to the nature of the cyberspace domain, Hollis

perceives that without the authority to synchronize the cyber efforts in one CCMD,

negative effects could quickly spread to another CCMD.[30] The aspect of command and

control that is a weakness for USCYBERCOM is its limited ability to harness unity of

effort. This occurs in two areas, the first is within the DoD, because the Services still

own their cyber capabilities. It will be up to USCYBERCOM to develop the processes

and controls to ensure that the Service cyber commands stay synchronized globally to

best support the requirements of the GCCs.

Finally, USCYBERCOM needs to address unity of effort with the other

government agencies and the private sector. In an article, Dr Richard Weitz discussed

this concern. "…[C]ertain analysts fear that CYBERCOM will so militarize U.S. cyber

defense efforts that the U.S. government will prove unable to realize the deep public-

private partnerships that experts see as essential for securing the internet."[31] The very

structure of USCYBERCOM itself creates an impediment to unity of effort. Combining

military and non-military intelligence assets (US Code Title 10[32] and Title 50[33]), under

one command intensifies perceived privacy concerns in the public and private sectors;

This is illustrated by the intense controversy over the former Bush administration global

wiretapping and message intercept programs.[34] The debate over perceived invasions of

privacy undermines USCYBERCOM's ability to achieve unity of effort. The next area of

discussion, computer network operations, will further explore these issues as another potential weakness for USCYBERCOM.

Computer Network Operations

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, defines Computer Network Operations as "Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations."[35] Ownership of Computer Network Operations (CNO) is elusive and is perhaps the area of weakness most important for USCYBERCOM strategy to resolve. Joint Publication (JP) 3-13, *Information Operations (IO)*, currently provides the only joint framework that addresses C2 for cyberspace war fighting. Joint doctrine contains no guidance for cyber force presentation. Information Operations (IO) doctrine defines computer network operations, comprised of computer network attack (CNA), computer network defense (CND), and computer network exploitation.[36] Until the creation of USCYBERCOM, the most glaring issue was that CNO's components-CND, CNA and CNE are not part of a single organization.

For the most part, the area of Computer Network Defense (CND) fell under the Defense Information Systems Agency (JTF-GNO) (disestablished by USCYBERCOM order[37]). The offensive functions developed and maintained by the intelligence community (JFCC-NW) (disestablished by USCYBERCOM order[38]); hide behind walls of classification with very limited access except for those organizations that maintain these capabilities. The NSA owns the highly classified area of CNE. In addition, the Services possess their own offensive capabilities independent of each other and the GCCs do not have the authorities to use them. With the establishment of USCYBERCOM, one

organization, on paper at least, gained responsibility for CNA/CND and under the dual-hat command relationship with DIRNSA gained responsibility over CNE.

USCYBERCOM must resolve its key CNO challenge of information sharing. It must create the mechanisms to share information across the military as well as U.S. government agencies and allies. One of the biggest obstacles is the classification of the different components of CNO, particularly within the Services. Most Service elements conducting CND do not have the capability or capacity to incorporate CNA and CNE at these lower levels. Their current facilities and organization do not support adding the highly classified information and operations these components. This is also the case when we look across the government and allies. As Weitz points out, "the security classification of NSA activities could impede the sharing of cyber security information among government agencies and with the private sector, which owns an estimated 90 percent of U.S. critical infrastructure."[39] The Center for Strategic and International Studies (CSIS) report also points to this current weakness, that it is easier to attack a collection of hierarchical stovepipes and harder to defend because our security programs are not of equal strength. Stovepiped defenders cannot appreciate the scope of, nor respond well to a multi-agency attack.[40] USCYBERCOM can be that solution but it will need to overcome the perception of need-to- know to one of collaboration and transparency.

The Services and the intelligence community are not in the habit of sharing information with each other. In a recent article, Deputy Secretary of Defense Lynn wrote,

> To facilitate operations in cyberspace, the Defense Department needs an appropriate organizational structure. For the past several years, the military's

cyberdefense effort was run by a loose confederation of joint task forces dispersed both geographically and institutionally. In June 2009, recognizing that the scale of the effort to protect cyberspace had outgrown the military's existing structures, Defense Secretary Robert Gates ordered the consolidation of the task forces into a single four-star command, the U.S. Cyber Command…[41]

His vision is that USCYBERCOM adapt active cyber defense using tools and procedures developed by the NSA. In his view, the cyber domain invites attack. As such, it needs coordinated defensive measures to allow internet users a safe global cyber environment.[42] What is interesting about his proposed strategy is that he did not mention the offensive capabilities of CNO. He depends on the Services for executing the active defense but does not discuss integrating the offensive components buried predominately in the intelligence community. In a recent Air Forces Times article, the author mentions that perhaps one of the key reasons for not discussing the offensive aspects of cyberspace is because there are still significant legal and strategic questions not yet answered.[43] USCYBERCOM will not be able to complete its comprehensive strategy until it finds a way to facilitate the free exchange of information among its CNO components.

There were two research papers recently written that scrutinize computer network operations. One of the notable findings and another subtle weakness for USCYBERCOM's strategy is the problem of control of CNO operations. COL Mahoney in his Program Research Project for the U.S. Army War College discusses the difficulties and need to develop a way to sub-delegate CNO authorities and capabilities to the GCCs. He references concern from GCC commanders in southwest Asia unable to convince national and DoD authorities to support their cyber offensive efforts.[44] Major Birdwell in his research project addresses the relationship, authorities and

responsibilities between the FCC and GCC. He advocates using USTRANSCOM, USSTRATCOM and USSOCOM as models to develop mechanisms to create regional CNO command and control between the two types of combatant commands.[45] As USCYBERCOM develops its emerging strategy, addressing this area will be significant, particularly when it comes to the next focus area, synchronization.

Synchronization

Synchronization of the varied elements of cyber is a daunting task. JP 1-02 defines synchronization as the arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. For USCYBERCOM, there are echelons of synchronization that it will need to master to produce the degree of security envisioned by senior leadership. The first level will be national level integration. One of the main purposes for the memorandum of agreement between Department of Homeland Security (DHS) and DoD is the need to synchronize cyber mission activities as they relate to U.S. cyber security.[46] The difficulty as written earlier will be overcoming hurdles in information sharing, particularly legal concerns surrounding Title 50 information. At the Service echelon, the difficulty is synchronizing cyber across the Doctrine, Organization, Training, Material, Leadership, Personnel and Facilities (DOTMLPF). To achieve synchronization, all DoD cyber capabilities must take direction from one organization and work together within a complex global domain that spans all physical domains. The order establishing USCYBERCOM suggests it must be capable of synchronizing warfighting effects across the global security environment. However, it does not expand its authorities and responsibilities for military cyberspace operations beyond those USSTRATCOM given in the UCP.[47] A good example that the

12

authority for synchronization is unclear is in the Army's *Cyberspace Operations Concept Capability Plan 2016-2028*. It directs that synchronization efforts need to take advantage of capabilities-based assessments, not just within the Army but also joint and national assessments. The document references the Army's assessment that it must go beyond its Service requirements and focus on joint needs, believing it has the responsibility to influence and design capabilities as it relates to the land.[48] This illustrates the ambiguity between what the individual Services and support agencies continue to believe is their scope of responsibility and what the DoD intended with the establishment of USCYBERCOM.

Last, the inability to synchronize DoD cyber efforts with global partners and private industry weakens both military and national cyber defense capabilities. Secretary Lynn in his article, *Defending a New Domain,* articulated this type of synchronization as USCYBERCOM's third mission.[49] USCYBERCOM's cyber strategy to defend the US can only succeed if it is coordinated across the government, allies and commercial sector partners.[50] Lynn argues that the decision to use military resources to support the private sector and U.S. allies will determine U.S. success in cyberspace.[51] In his article, Dr Weitz also noted that U.S. officials agreed that they need extensive cooperation with non-DoD partners in government, industry, and academia as well as in foreign countries.[52] *The Cyberspace Policy Review* discussed one of the complexities of synchronization with the private sector. The review describes how a government partnership needs to delineate roles and responsibilities, integrate capabilities, and take ownership of the problem to develop holistic solutions.[53] The primary obstacle, which may be negatively influencing the government's relationship with the private sector, is

the perceived potential for the militarization of cyberspace. To ensure the success of USCYBERCOM's strategy, it is vitally important for the US government to form an open partnership with the private sector, which has the knowledge, skills, and resources that the government lacks.

Resourcing

The final aspect that could hinder cyber security efforts is resourcing. USCYBERCOM needs to hire cyber professionals, train both the current military and civilian work force, and fundamentally change our acquisition processes. The big question is where will USCYBERCOM find the resources and how will it adapt to the current environment of reduced resourcing. In General Alexander's testimony to congress in SEP 2010, he mentioned that the command would grow to 1100 personnel.[54] The personnel needed by USCYBERCOM will take time to hire. Public and private employers are heavily dependent on and seek to hire from the same limited pool of cyber security experts and other skilled IT/cyber professionals.[55] Secretary Lynn described the human capital challenge in an even more worrisome way. He wrote that as the U.S. tries to grow this cyber work force it only possesses, "4.5 percent of the world's population, and over the next 20 years, many countries, including China and India, will train more highly proficient computer scientists than will the United States."[56]

Another resource challenge is cyber funding. At the national level, there is loose oversight by the Office of Management and Budget over funds designated for cyber security. In addition, divided federal funding lines lead to fragmentation as each agency receives its own funding for IT budgets and buys its own equipment.[57] Within the DoD, cyberspace basic funding for CNO is broken up between the Services and support

14

agencies. The *Comprehensive National Cyberspace* initiative provides supplemental funding but does not provide guidance on the funds' use.[58] This adds additional complexity to coordinating resources for cyber security. USCYBERCOM must develop oversight authority to synchronize diverse funding into a cohesive long- term plan that will maximize the dollars allocated to cyber security.

Finally, USCYBERCOM's strategy must address the acquisition process. Simply put, the government's acquisition process is too cumbersome and lengthy to be of any help to USCYBERCOM's cyber strategy. According to Secretary Lynn, it takes the DoD 81 months to field a new computer system once funded. It took Apple 24 months to develop and field the iPhone, less time than it takes the Pentagon just to get a system approved by congress.[59] To be effective in cyberspace, DoD needs to revamp its acquisition cycle in order to maintain pace with the IT industry. The 2010 QDR addressed this issue with a directive that the Pentagon develops a faster IT process.[60] Without change to resourcing processes, USCYBERCOM's cyber strategy will continue to be at risk.

Recommendations

To achieve real progress, USCYBERCOM must focus on organization, command and control, computer network operations (CNO), synchronization, and resourcing. There are three clear recommendations that if addressed by senior leadership will allow forward movement on a strong viable cyberspace strategy. The first recommendation is to transition USCYBERCOM to a separate functional combatant command based on the USSOCOM model. This modification would expand USCYBERCOM's authorities and responsibilities, facilitating its development of the global cyberspace operational

capability envisioned by national strategic guidance. USSOCOM has Title 10 authority

over all DoD special purpose forces. For USCYBERCOM, gaining the same ability to

train and equip the very limited DoD global cyberforce would provide significant

advantage in standardization, synchronization, and effective command and control.[61] To

be successful this needs to include the highly classified CNA and CNE assets. This

change benefits the unified commands by providing a fully integrated and functional

global computer operations structure. A USSOCOM model allows USCYBERCOM to

improve geographic support by reorganizing to a regionally aligned command instead of

its current Service based structure. This would eliminate the potential inter Service/

Agency competition for cyber resourcing. Unless USCYBERCOM succeeds, its ability

to influence the limited resources available to the Services for cyber security will

continue to impact operational and force management risk areas.[62]

Second, USCYBERCOM and DoD must resolve cyber command and control.

The line and block charts of current joint and Service doctrine provide the basic

operational relationships of OPCON, TACON and ADCON.[63] Within the global cyber

domain, no clear doctrine currently exists which outlines the technical relationships

necessary to provide C2 of global cyber operations. The creation of doctrine needs to

be a priority to clearly define and organize the technical C2 of DoD cyber elements into

an effective and reliable element of combat power. MAJ Birdwell in his papers regarding

CNO operations proposes that creating theater (regional) sub-unified commands similar

to USSOCOM improves the FCC/GCC command and control relationship. He argues

that creating a structure of regionally aligned CNO commands nests well for the global

CNO mission while directly supporting the GCC requirements on a day-to-day basis.[64] In

COL Mahoney's paper, he also perceives issues with CNO at the strategic level; including both legal and policy issues and the command and control relationship to the GCC. His analysis, influenced by Major Birdwell, came to a similar conclusion that within the GCCs there needs to be a regional CNO element for command and control. He also wants to see authority for cyber actions delegated to the local CNO element, providing the GCC with actionable cyber capabilities. In regards to the issue over the dual hat relationship, COL Mahoney recommends that the commander of USCYBERCOM needs to be a former GCC commander, but that he stays dual-hatted as the DIRNSA.[65] This may be the best solution to concerns of a dual-hatted commander. The course of action ensures the CNE function and Title 50 elements of CNO remain consolidated in USCYBERCOM, and diminishing the concern over bias that an Intel Community commander brings. If USCYBERCOM's strategy does not resolve global technical command and control, it will not own the ability to operationalize its cyber force to meet the demands of the GCCs. This increases operational risk to the DoD's future ability to deter or defeat emerging cyber threats.

Third, USCYBERCOM must assume control and oversight of cyber resources within the DoD and needs to become a partner in determining where other national cyber resources are applied. A unique facet of the USSOCOM model is the fact that congress established a new category of funding (Major Force Program 11) for them, and the authority to train and equip forces.[66] COL Hollis argues that USCYBERCOM, with similar funding and acquisition authorities can streamline and coordinate military cyberspace capabilities, as opposed to the Services fielding uncoordinated and disjointed capabilities.[67] A congressional funding action would make it possible to

provide USCYBERCOM control of all agency cyber funding and oversight of cyber

intelligence appropriations for CNA/ CNE. The overall advantage is that one

organization could provide the crucial oversight of the fragmented national and DoD

cyber- related funds, to include those provided to the Services.

Allowing USCYBERCOM to manage all cyber resources across DoD would

provide the control necessary to standardize and integrate cyber capabilities across the

DoD, producing synergy and cost savings that the current resourcing structure does not.

One negative consequence of such a change would be reduced control by Service and

agency leadership over those realigned resources. Another consequence is the time it

will take to make these changes through the current DoD and congressional

processes.[68] The risk of giving USCYBERCOM such autonomy is that it might reinforce

the perception that the US government is militarizing cyberspace.

Conclusion

This paper examined five aspects of USCYBERCOM: organization, command

and control, computer network operations (CNO), synchronization, and resourcing.

Each has specific areas that impede development and implementation of a viable cyber

security strategy within the Department of Defense. Of these, difficult changes to

organization, command and control, and resourcing will have the most impact on

USCYBERCOM's ability to mature a comprehensive strategy that will provide the unity

of effort necessary to succeed in the cyber domain. The recommendations made are an

analysis of current thought on both published policy and guidance for the DoD and other

government agencies developed over the last decade. Achieving these

recommendations will require forward thinking and difficult decisions by military senior

leaders. The obstacles they face are daunting. The CCMDs, Services, and agencies developed their own capabilities and want to maintain their independence. Senior leaders must overcome this resistance as well as overcoming OSD staff and congressional hurdles.[69]

Research for this paper brought to light some additional concerns that may further affect national security efforts in the realm of cyberspace. The research pointed to several general perceptions that may influence future decisions, including concern over Title 50 intelligence collection, Federal Information Security Act (FISA), changes to the Patriot Act, and concern over domestic information collection. Research also shows that there is an opposing viewpoint, which questions whether cyber is a true national strategic security risk. Jean-Loup Samaan writes, "far from solving the policy concerns surrounding cyber-defense the creation of Cyber Command displays a lack of consensus within the defense community on the threat assessment of cyberspace and its military implications."[70] In another article he argues, "… that getting the strategic appraisal right should be the priority when designing relevant military Posture."[71] An environment with varying degrees of commitment to cyber security will challenge USCYBERCOM leaders as they attempt to link diverse elements of cyber into an effective and efficient security strategy for an uncertain future.

Endnotes

[1] Richard Mesic et al, *Air Force Cyber Command (Provisional) Decision Support*, (Santa Monica, CA: Rand Corporation, 2010), iii-iv, http://www.rand.org/pubs /monographs /2010/RAND_MG935.1.pdf (accessed 12 February 2011). Discusses the perceived leadership of the Air Force in Cyber and discusses the implications of adding Cyber to its mission statement in 2005. Completed in 2008 but not published until 2010.

[2] U.S. Secretary of Defense Robert M Gates, "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations," memorandum for Secretaries of the Military Departments, Washington, DC, July 23, 2009.

[3] James R. Langevin et al, *Securing Cyberspace for the 44th Presidency*, (Washington, DC: Center for Strategic and International Studies, December 2008), 12, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf (accessed 18 December 2010).

[4] George W. Bush, *National Strategy to Secure Cyberspace*, (Washington, DC: The White House, February 2003).

[5] Tom Gjeltne, "Cyber Insecurity: U.S. Struggles to Confront Threat," *National Public Radio*, 10 April 2010 and "Timeline: Major Cybersecurity Incidents since 2007," *National Public Radio*, 5 April 2010, http://www.npr.org/templates/story/story.php?storyId= 125578576 (accessed 28 April 2011) and Langevin et al, *Securing Cyberspace for the 44th Presidency,* 12.

[6] Ben Bain, "Number of Cyber Incidents Jumps," *Federal Computer Week*, 17 February 2009, http://fcw.com/Articles/2009/02/17/CERT-cyber-incidents.aspx (accessed 26 April 2011).

[7] George W. Bush, *National Security Strategy*, (Washington, DC: The White House, March 2006), 44.

[8] Barack H. Obama, *National Security Strategy*, (Washington, DC: The White House, May 2010), 27-28.

[9] U.S. Secretary of Defense Donald Rumsfeld, *Quadrennial Defense Review Report*, (Washington, DC: U.S. Department of Defense, 6 February 2006), 50-51.

[10] Chairman of the Joint Chiefs of Staff Peter Pace, *National Military Strategy for Cyberspace Operations*, (Washington, DC: Department of Defense, December 2006).

[11] Ibid.*,* 19.

[12] Langevin et al, *Securing Cyberspace for the 44th Presidency,* 1.

[13] Ibid., 36.

[14] The White House, "Cyber Policy Review Assuring a Trusted and Resilient Information and Communications Infrastructure," (Washington, DC: The White House, May 2009), http://www.whitehouse.gov/assets/documents/ Cyberspace_Policy _Review_final.pdf (accessed 18 December 2010).

[15] Pace, *National Military Strategy for Cyberspace Operations,* v.

[16] David M. Hollis, USCYBERCOM: The Need for a Combatant Command versus a Subunified Command, Joint Force Quarterly: JFQ, no, 58, (3rd Quarter 2010): 51, in ProQuest , (accessed 27 September 2010).

[17] Pamela Hess, "Pentagon Puts Hold on USAF Cyber Effort," *Associated Press*, 13 August 2008, http://www.usatoday.com/news/washington/2008-08-13-4204192373 _x.htm (accessed 18 December 2010).

[18] Gates, "*Establishment of a Subordinate Unified U.S. Cyber Command,"* 1.

[19] Ibid., 3.

[20] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, Joint Publication 1 (Washington, DC: Joint Chiefs of Staff, 2 May 2007, Incorporating Change 1, 20 March 2009), II-5.

[21] Hollis, "USCYBERCOM: The Need for a Combatant Command," 51.

[22] Keith B. Alexander, "United States Cyber Command," in, *Cyber Defense, The U.S. Military Prepares for 21st Century Electronic Warfare and Cyber Terrorism*, ed. Sidney E. Dean (Transatlantic Euro-American Multimedia LCC, 2nd Edition, 5 October 2010), kindle e-book.

[23] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces,* II 5-II 7.

[24] Richard Weitz, "Department of Defense Prepares for CYBERWAR The Current State of Play" *Second Line of Defense (SLD)*, 12 April 2011, 3, http://www.sldinfo. com/? p=17302 (accessed 12 April 2011).

[25] Ibid., 2.

[26] Keith B. Alexander, "United States Cyber Command," in, *Cyber Defense*.

[27] Bodine M. Birdwell and Robert Mills, *"*War Fighting in Cyber Space Evolving Force Presentation and Command and Control*," Air and Space Power Journal,* 25, no. 1, Spring 2011, http://www.airpower.au.af.mil (accessed 13 April 2011), 26-34.

[28] Hollis, "USCYBERCOM: The Need for a Combatant Command," 51.

[29] Bodine M. Birdwell, *If You Don't Know Where You Are Going, You Probably Will End Up Somewhere Else. Computer Network Operations Force Presentation,* (Wright-Patterson Air Force Base, OH: Air Force Institute of Technology, June 2009), 8.This author's review of joint doctrine indicates US Strategic Command should consider adopting specific lessons learned from the force presentation and C2 for space, logistics and special operations. Adoption of these lessons learned should make CNO force presentation and C2 more capable, efficient, and integrated within the DoD warfighting construct.

[30] Hollis, "USCYBERCOM: The Need for a Combatant Command," 51.

[31] Weitz, "Department of Defense Prepares for CYBERWAR," 5.

[32] *The Armed Forces*, United States Code Title 10, CH. 1041, SEC. 1, 70A (10 August 1956). http://uscode.house.gov/download/title_10.shtml (accessed 12 February 2011).

[33] *War and National Defense*, United States Code Title 50, (1 February 2010), http://uscode.house.gov/download/title_50.shtml (accessed 23 April 2011)

[34] Weitz, "Department of Defense Prepares for CYBERWAR," 6.

[35] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, (Washington, DC: US Joint Chiefs of Staff, 12 April 2001, as amended through 13 June 2007), 111.

[36] U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13, (Washington, DC: Joint Chiefs of Staff, 13 February 2006), IV-5.

[37] Robert M. Gates, "*Establishment of a Subordinate Unified U.S. Cyber Command,*" 3.

[38] Ibid., 3.

[39] Weitz, "Department of Defense Prepares for CYBERWAR," 6.

[40] James R. Langevin et al, *Securing Cyberspace for the 44th Presidency*, 41.

[41] William J Lynn III, "Defending a New Domain," *Foreign Affairs*, 89, no. 5, (September/October 2010), in ProQuest (accessed 4 November 2010).

[42] Lynn, "Defending a New Domain."

[43] Ibid.

[44] John R. Mahoney, *Reflections on a Strategic Vision for Computer Network Operations*, Program Research Project (Carlisle Barracks, PA: U.S. Army War College, 25 May 2010), 21-22.

[45] Birdwell, *If You Don't Know Where You Are Going*, 6-7.

[46] U.S. Director of Homeland Security Janet Napolitano and U. S. Secretary of Defense Robert M. Gates, "Memorandum of Agreement Between the Department of

Homeland Security and the Department of Defense Regarding Cyber Security," parties to the agreement are the Department of Homeland Security (DHS) and Department of Defense (DOD), (Washington, DC: Department of Homeland Security and Department of Defense, 13 October 2010), 1.

[47] Robert M. Gates, "*Establishment of a Subordinate Unified U.S. Cyber Command",* 1-3; George W. Bush, "*The Unified Command Plan,*" (Washington, DC: The White House, May 2006), 12 http://www.dod.gov/pubs/foi/ojcs/08-F-0518.pdf (accessed 12 May 2011).

[48] U.S. Department of the Army, *The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028,* (Washington, DC: Department of the Army, 22 February 2010), 57.

[49] Lynn, "Defending a New Domain."

[50] Ibid.

[51] Ibid.

[52] Weitz, "Department of Defense Prepares for CYBERWAR," 5.

[53] The White House, "Cyber Policy Review," 17.

[54] Keith B. Alexander, "United States Cyber Command," in *Cyber Defense*.

[55] Weitz, "Department of Defense Prepares for CYBERWAR," 2.

[56] Lynn, "Defending a New Domain."

[57] Hollis, "USCYBERCOM: The Need for a Combatant Command," 51.

[58] National Security Council, (January 2008).*Comprehensive National Cyberspace Initiative,* http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed 2 May 2011).

[59] Lynn, "Defending a New Domain."

[60] U.S. Secretary of Defense Robert M. Gates, *Quadrennial Defense Review Report*, (Washington, DC: U.S. Department of Defense, February 2010), 93.

[61] Womble, Cynthia, "Transforming USTRANSCOM: Is USSOCOM a Model?," *Army Logistician*, 35,2, (March/April 2003): 37, in ProQuest (accessed 12 May 2011).

[62] Gates, "Quadrennial Defense Review Report," 89-90. Gates describes risk as operational, which includes the ability of the current force to execute strategy within acceptable cost. Force management risk includes ability to recruit, train, equip and

sustain for the near, mid and long term. The institutional risk includes the capacity of management and business practices to plan, enable and support DoD missions. Risk to future challenges encompasses the capacity to execute future missions successfully and hedge against shocks.

[63] U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0, (Washington, DC: US Joint Chiefs of Staff, 17 September 2006, change 2, 22 March 2010), II 6-9.

[64] Birdwell, *If You Don't Know Where You Are Going*, 55-56. Author provides a very detailed analysis. Recommend reading the complete document for better understanding of the FCC/GCC relationship issues that need resolution.

[65] Mahoney, *Reflections on a Strategic Vision,* 24-25.

[66] Womble, Cynthia, "Transforming USTRANSCOM: Is USSOCOM a Model?," 34.

[67] Hollis, "USCYBERCOM: The Need for a Combatant Command," 51.

[68] Ibid., 52.

[69] Ibid., 49.

[70] Jean Loup Samaan, "Cyber Command the Rift in US Strategy," *The RUSI Journal*, 155: 6, (22 DEC 2010): 16, http://www.rusi.org/publications /journal/ref:A4CFE1E40D3643 (accessed 14 February 2011).

[71] Jean Loup Samaan, "Beyond the Rift in Cyber Strategy," *Strategic Insights*, 10, no.1 (Spring 2011): 11, http://www.nps.edu/Academics/Centers/CCC/Research-Publications/StrategicInsights/index.html (accessed 28 April 2011).